THE DIR CYBERSECURITY INSIGHT

August FY2016 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

Want Help Getting Funded? Here's How!

"You can't always get what you want

You can't always get what you want

But if you try sometimes you just might find

You get what you need"

The Rolling Stones song, "You Can't Always Get What You Want," was released in July 1969. Although the world looks vastly different now than it did in 1969, the song still has merit in 2016. Preparations for the 2017 Legislative Session are well underway and we are all focusing on what we need to keep our security programs running smoothly and what we want to improve and mature those programs.

Working in the public sector, you may get some of what you need and a sliver of what you want. But you won't get what you don't ask for.

The Legislature has seen an increase in the number of requests for cybersecurity related items, as well as a need to replace legacy systems. They charged DIR with submitting a prioritization for items relating to cybersecurity and legacy systems modernization.

More specifically, under section 9.10 of the General Appropriations Act, Prioritization of Cybersecurity and Legacy System Projects[1], the legislature required DIR to submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the October 2014 Legacy Systems Study, to be considered for funding to the Legislative Budget Board (LBB) by **October 1, 2016**.

Agencies were asked to coordinate and cooperate with DIR to implement this provision. The PCLS module in SPECTRIM provides agencies with the ability to demonstrate the risks and impact of cybersecurity and legacy projects that are not funded. DIR will use these responses to determine the prioritization that will be sent to the LBB.

If your agency is requesting funding for cybersecurity or modernizing legacy systems, you must complete the online assessments using the SPECTRIM (Archer) portal to be included in the prioritization report. Each agency will need to complete all assessments by their LAR submission deadline. This is how you can ask for what you 'want' from the legislature and explain why you 'need' it.

DIR has provided resources for assisting you in this process that can be accessed on the Prioritization of Cybersecurity and Legacy Systems (PCLS) webpage. Any specific questions can be directed to PCLS@dir.texas.gov.

CONTENTS

[1] **Sec. 9.10. Prioritization of Cybersecurity and Legacy System Projects.** Out of funds appropriated elsewhere in this Act and in accordance with Government Code, Chapter 2054, the Department of Information Resources (department) shall submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the October 2014 Legacy Systems Study, to be considered for funding to the Legislative Budget Board by October 1, 2016. Agencies shall coordinate and cooperate with the department for implementation of this provision.

A Round of Applause

DIR is pleased to announce that its SPECTRIM (Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management) portal was a finalist in the 2016 NACIO State IT Recognition Awards! Congratulations to Eddie Block, the state CISO, Nancy Rainosek, the state administrator for the SPECTRIM portal, and the OCISO team on achieving this recognition!

InfoSec Academy Update

The InfoSec Academy is now live! DIR is proud to be partnering with New Horizons for this endeavor. The Academy offers several libraries of courses and resources for On Line Anytime learning (OLA) along with On Line Live (OLL) certification preparation courses. The Texas Security Policy and Assurance course is required before taking any of the OLL certification preparation courses. This course offers both a computer-based OLA course, and as an Instructor-Led Training (ILT) course.
Upcoming ILT classes are scheduled from 8:00 to 4:00 on the following days:

August 12, 2016

September 16, 2016

November 21, 2016

January 16, 2017

The OLA version of the Texas Security Policy and Assurance course is now available!

Instruction will occur at the New Horizons Austin location: 300 E Highland Mall Blvd, Suite 100 - Austin, TX 78752. If you would like to sign up, VISIT THE INFOSEC ACADEMY website. If you have any questions about the InfoSec Academy, visit our website or send an email to infosecacademy@dir.texas.gov.

NSOC Update

The NSOC is constantly working on proof of concepts (POC). One of our key functions is to evaluate new and emerging security tools. POCs are conducted prior to adding in a new capability at the NSOC. This process can be a lengthy proposition when evaluating multiple vendors and tools. While we are always open to share more specific results on a type of technology that we have evaluated with you one on one, it may be helpful to provide some detail on how the NSOC structures its POCs (listed below). We hope sharing this information will help you on your next POC.

- **What is a POC?**
  - A POC is a formal evaluation of multiple products or processes to determine viability in your environment.
- **Why should you do a POC?**
  - Your team has decided either from internal feedback or external reviews/input that there is a gap in the current security posture.
  - Your organization would like to stay current on technology
  - You can evaluate multiple vendor solutions
  - You can gatherevidence of value to support a purchasing decision
- **When to do POCs**
  - The POC should support the security program and attempt to add a technology or process that is needed.

- While POCs don't necessarily result in procurement, they should be scheduled in accordance with funding cycles in the eventuality a viable solution is found
- The POC should be scheduled after careful consideration of all vendors in the market space (Gartner and others can speed this process up for you)
- When you have the time(depending on technology these can take up to 30-90 days to complete)

- **Process for completing a POC**
  - Identify a potential technology to evaluate
  - Identify potential vendors providing the solution
  - Develop your success criteria (short and long term)
  - Select candidates for your evaluation
  - Schedule accordingly (30-90 days; build in some white space as vendors don't always deliver on time and/or issues arise with new equipment)
  - Be intentional about overlapping evaluations
- **Other considerations**
  - A POC does not necessarily result in a procurement
  - Look for external validation of vendor success; previous success with other clients does not guarantee a good fit for you (consider similar customers, i.e. state agencies)
  - Develop success criteria carefully
    - Performance: does the technology do what its supposed to?
    - Compare vendor support categories, maintenance, training, set-up, customizations
    - Total cost of ownership
    - Weight of success criteria for a quantitative outcome

Roses are Red, Violets are Blue…

On October 15, your SPT is due…..

That's right! Each agency and higher education institution is required to submit their security plan template to DIR on October 15 of even numbered years. The data from 2014 is loaded into the SPECTRIM portal so that you can use that as your foundation for this year's plan. You can find information about the SPT on the DIR website here. You can find information about the SPECTRIM portal here.

Information Security Officer Spotlight

Monty Black, CompTIA Network +, MSCE, CISSP
Information Security Officer
Texas Department of Information Resources

I am the ISO/COOP Coordinator for the DIR. Providing services for the citizens of Texas as well all of the state agencies is rewarding and challenging. DIR's focus on forward thinking and innovation creates an environment that makes every day interesting, especially from a security perspective.

Tell us how information security has changed since you started in your role.

As the nature of exploitation has evolved, so has the role of information security. In the early days, security was often an afterthought or occurred only as a reaction to a disruptive event. Today, it is becoming integrated into every aspect of technology.

Who are your customers, and what is one of the most challenging areas for you?

From an organizational perspective, DIR is divided into DIR-A and DIR-E. DIR-E is the outward facing enterprise security team interfacing with other state agencies and higher education entities. DIR-A is internal serving DIR staff. I also provide security guidance to the digital government team that runs the Texas.gov program, so in that sense, my customers are the citizens of Texas.

How did you come into the security field?

I've been interested in computer security from the first moment I used a dial up connection to access my university's computer network. The second I connected to another computer that responded to my commands, the possibilities for mischief seemed infinite. I began reading anything I could find on networks and information security. With the advent of the WWW, other forms of malware became very prevalent and my experience with viruses often led to my performing clean up, containment jobs and other security functions, for various small business customers. When I began working for the state, I was asked to handle desktop security and administration of the anti-virus servers for my agency. I eventually began working with the security team at the agency, doing incident response duties and computer forensics. Finally, in 2012, I transitioned from system administration to a full time security role.

Top 3 life highlights

1. Birth of my son
2. Hearing a song I wrote air on the radio
3. Moving to Texas

People would be surprised to know:

I am a professional musician and song writer. I've had songs I've written / co-written appear on the Texas music charts as well XM Radio.

Which CD do you have in your car? Or what radio station do you listen to?

AC/DC - T.N.T.

If you could interview one person (dead or alive) who would it be?

Winston Churchill

If given a chance, who would you like to be for a day?

Probably Bill Gates…I'd mail my other self a big check!

What is the best advice you have received and that you have used?

When the chips are down, keep working. Work will get you through most things.

What would be your advice for a new security professional?

"Compromise is the Art of Kings" a line I've blatantly stolen from the movie Braveheart. In the security world, I've found that the need for security must be communicated and always striven for, but one can never lose sight of the complexities of technology and the imperative to make systems more functional, user friendly and efficient. It's a balancing act.

Insight from our Texas CISO

Eddie Block
CISO, State of Texas

"By failing to prepare, you are preparing to fail."

-- Benjamin Franklin

Incident response, disaster recovery, continuity of operations, succession plans… the list goes on. In the security world there is no shortage of plans. We prepare for worst case scenarios, hoping that we will be ready if and when that scenario comes to pass. Security practitioners tend to be a paranoid bunch (yes, I'm looking at you). We are also very creative and can come up with some amazing disaster scenarios.

We can't prepare for every situation, though. I've seen disaster recovery plans that attempt to address very rare occurrences but ignore simple risks. These plans consider electromagnetic pulses from solar flares, but ignore the fact that the hot water pipes run in the plenum over the data center. A plan that is too creative can end up missing the mark. We have to look at risk factors: likelihood and impact.

What is the likelihood of an earthquake in Texas or a meteor crashing on my building? Sure, there is the possibility that something cataclysmic will happen, but how likely is it? It is more likely that a hurricane will come through Texas than a volcano will erupt. We need to plan for the simple and likely occurrences like power outages, physical theft and suicidal squirrels (please visit http://cybersquirrel1.com/ if you don't believe me).

What is the impact of a flooded data center or someone accidentally hitting the big red button that kills power to the datacenter instead of the one that opens the door? Yes, I've seen these two buttons next to each other. Whether the outage is caused by human error, natural disaster or those squirrels, the impact is the same. So why do we spend time worrying over meteors?

We have attempted to make the risk assessment process less daunting with our SPECTRIM Risk Management module. You can perform an assessment on your data center once, then systems in that data center inherit risks, controls, and mitigations. Each new system becomes easier to assess in relation to the environment. We hope that this system will make risk no longer a four-letter word.

"In preparing for battle I have always found that plans are useless, but planning is indispensable."

-- Dwight D. Eisenhower

There is great value in the planning process. A few years ago DHS utilized pop-culture fascination with zombies to build awareness around preparedness. They issued an entire campaign about preparing for the zombie apocalypse, knowing that the same preparations would be valuable in a flood, hurricane, blizzard, power outage, etc. While we might not be able to sell zombies to our leadership, focusing on likely events with great impact should help bolster our preparations across the board.

Eddie Block
CISO, State of Texas

Events

2016 Save the Dates

- Monthly Gartner Webinar: "State of the Threat Environment 2016"
  Tuesday, August 9, 10:00 AMs central time
- 2016 TASSCC Annual Conference: August 7 – 10, Galveston, TX
- 2016 NSA Information Assurance Symposium (IAS): August 16– 18, Washington, DC
- CyberTexas Summit: August 23 – 24, San Antonio, TX
- MS-ISAC Annual Meeting: October 30 – November 2, San Antonio, TX
- Innotech Austin: November 17, Austin, TX